Enhanced delegated computing using coherence

Enhanced delegated computing using coherence

Stefanie Barz,[1] Vedran Dunjko,[2,3] Florian Schlederer,[1] Merritt Moore,[1] Elham Kashefi,[4,5] and Ian A. Walmsley[1]
[1]*Clarendon Laboratory, Department of Physics, University of Oxford, OX1 3PU, United Kingdom*
[2]*Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Technikerstrasse 21a, A-6020 Innsbruck, Austria*
[3]*Institute for Theoretical Physics, University of Innsbruck, Technikerstrasse 25, 6020 Innsbruck, Austria*
[4]*School of Informatics, Informatics Forum, 10 Crichton Street, Edinburgh, EH8 9AB, United Kingdom*
[5]*Laboratoire Traitement et Communication de l'Information CNRS - Télécom ParisTech, 23 Avenue d'Italie 75013 Paris, France*
(Received 14 December 2015; published 28 March 2016)

A longstanding question is whether it is possible to delegate computational tasks securely—such that neither the computation nor the data is revealed to the server. Recently, both a classical and a quantum solution to this problem were found [C. Gentry, in *Proceedings of the 41st Annual ACM Symposium on the Theory of Computing* (Association for Computing Machinery, New York, 2009), pp. 167–178; A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 2009), pp. 517–526]. Here, we study the first step towards the interplay between classical and quantum approaches and show how coherence can be used as a tool for secure delegated classical computation. We show that a client with limited computational capacity—restricted to an XOR gate—can perform universal classical computation by manipulating information carriers that may occupy superpositions of two states. Using single photonic qubits or coherent light, we experimentally implement secure delegated classical computations between an independent client and a server, which are installed in two different laboratories and separated by 50 m. The server has access to the light sources and measurement devices, whereas the client may use only a restricted set of passive optical devices to manipulate the information-carrying light beams. Thus, our work highlights how minimal quantum and classical resources can be combined and exploited for classical computing.

DOI: 10.1103/PhysRevA.93.032339

I. INTRODUCTION

The storage and processing of data on remote servers has become highly relevant to modern information processing [1]. With the progress from stand-alone machines to large connected networks, the security of delegated computations has become increasingly important. In 2009, a classical scheme, the fully homomorphic encryption protocol, was invented which provides computational security in data processing at remote servers [2]. At the same time, a quantum computing protocol was found which allows an almost-classical client to delegate a quantum computation securely to a quantum server [3,4]. In contrast to the classical algorithm, the quantum version provides unconditional security [3,5–7].

Here, we study the first step towards the interplay between classical and quantum delegated computation [8,9]. To this end, we consider a game setting with a restricted client with access to only an XOR gate. We then explore what additional resources enable the client to delegate the secure computation of a NAND gate to an untrusted server. A similar (noncrypto) setting has been also explored recently to highlight the role of quantum contextuality [10] and quantum correlation [11] in boosting linear classical computation (done by XOR gates) to a nonlinear classical computation (done by NAND gates). Furthermore, it has been used to study multiparty cryptographic settings in [12] and the relation of entangled quantum states and multiparty computational games in [13].

In this paper we show that secure delegated NAND computation can be accomplished using *cobits*, short for *systems capable of being in a coherent superposition of two states* (see Fig. 1), for example, single photonic qubits or coherent laser beams. In our scheme, the server has access to cobits and the client is restricted to parity computations and the local manipulation of the cobits. The protocol works in the following manner: The server sends cobits, and the client applies simple operations to them, dependent on the classical bits the client wants to compute the NAND gate on. The cobits are then sent back to the server, which performs a measurement. The result contains the encrypted outcome of the NAND operation performed on the client's classical bits. This means that the cobit enables the client to compute problems beyond her own power, since the NAND gate is universal for classical computation. We note that the word *cobit* was introduced in another context with a different meaning [14], where it referred to a type of physical process which can convey a cobit of information. In our context *cobit* means a physical carrier of information, which can store two orthogonal states or fields and a (equally weighted) coherent superposition of the two.

Further, we experimentally implement a classical secure delegated computation by using single qubits or coherent laser beams as cobits. In our implementation, the client and the server are set up in two different laboratories, separated by more than 50 m and connected by optical fibers. Photonic systems are ideally suited for this task, since they can be easily manipulated and transmitted over large distances; however,

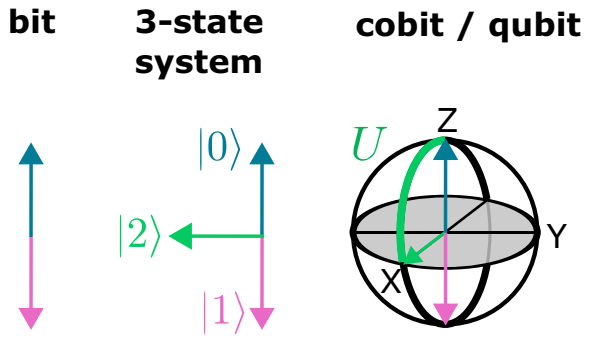

FIG. 1. Bits, three-state systems, cobits, and qubits. Our secure delegated computing protocol can be achieved by means of a three-state classical system. It can also be accomplished using cobits and qubits, which are two-state systems capable of being in a coherent superposition of both states. Here, the operation U transforms basis states into superposition states and vice versa. In the context of this work, cobit means a physical carrier of information, which can store two orthogonal states or fields and coherent superpositions of the two, for example, coherent laser beams. Qubits are quantum systems and can be realized experimentally, for example, by using different degrees of freedom in single photons. Thus, encoding information in a classical light beam's polarization would constitute a cobit, whereas doing the same with single photons realizes a qubit.

our scheme can be implemented using every physical system that provides coherence.

II. THEORY

Our work is based on a protocol for secure delegated classical computation using quantum resources [8]. It was shown that manipulating only two-level bits are not sufficient for this task. Here, we reformulate the original work [8] and show that in the same setting adding classical coherence enables us to perform secure delegated classical computations.

The protocol is based on the implementation of a NAND gate using only parity computations and coherence. Here, we first describe the protocol using single cobits and show later its implementation with single photonic qubits and coherent beams, which relaxes the requirements of the initial theory [8]. In detail, the protocol works as explained in the following (see also Fig. 2). First, the server generates cobits in the state $|0\rangle$ and sends these cobits to the client. The client wants to implement a NAND gate on two input bits a and b. Therefore, the client encodes the result of a NAND(a,b) gate in the output cobit by applying the gate sequence

$$|\mathrm{NAND}(a,b)\oplus 1\rangle = (U^\dagger)^{a\oplus b}U^bU^a|0\rangle. \quad (1)$$

Here, U is an operation which brings the state $|0\rangle$ into a superposition of $|0\rangle$ and $|1\rangle$. If U is applied to the superposition of $|0\rangle$ and $|1\rangle$, the cobit will be in state $|1\rangle$ after the operation $(U(U|0\rangle) = |1\rangle)$. In our protocol, the application of the operation U is controlled, depending on the values of a and b. Only if $a = b = 1$ is the output cobit in state $|1\rangle$; for all other settings of a and b, the output cobit is in state $|0\rangle$. Thus, the output cobit can be written as $|\mathrm{NAND}(a,b)\oplus 1\rangle$ and effectively contains a NAND gate.

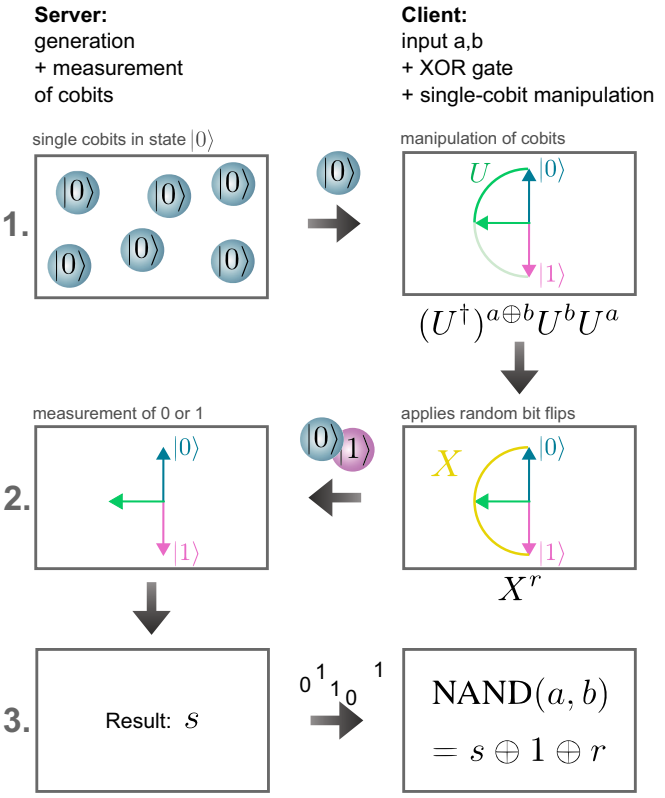

FIG. 2. Scheme of delegated NAND gate. The steps of the protocol are described in detail in the main text.

In order to hide the state of the output cobit and achieve secure delegated computing, the client applies an additional random bit flip X:

$$|\mathrm{NAND}(a,b)\oplus 1\oplus r\rangle = X^r|\mathrm{NAND}(a,b)\oplus 1\rangle, \quad (2)$$

where r is a random value.

The cobit is then sent back to the server, where a measurement in the $|0/1\rangle$ basis is performed. The result of this measurement, s, is returned to the client, who finally obtains the result NAND(a,b) by computing

$$\mathrm{NAND}(a,b) = s\oplus 1\oplus r. \quad (3)$$

A. Relation to previous work

We note that a NAND computation, without considering the security aspects, was first proposed in another work [11]. There, a classical parity computer controlled three-qubit Greenberger-Horne-Zeilinger states in order to perform universal classical computation in a measurement-based version fashion [15,16].

Reference [8] shows that a NAND computation can be performed using single qubits. Even more, it shows that computation can be performed in a secure client-server setting if the server has access to single qubits and the client to controlled single-qubit gates and an XOR gate.

Our work shows that the same functionality can be achieved without having any quantum resources at all. Compared to [8], we show that the resources required for a NAND computation can be reduced from single qubits to systems capable of being

in a coherent superposition of two states, *cobits*. Furthermore, we achieve secure delegated computations by sending cobits. In our framework, the server needs to have access to cobits, for example, coherent laser beams of single photons; the requirements for the clients are the same as the ones in [8]. This reduction to the manipulation of "simple" resources, compared to the generation of entanglement, clearly decreases the experimental requirements and enables one to perform secure and delegated classical computations with minimal resources.

III. IMPLEMENTATION

All systems that allow for a coherent superposition of two states can be used as resources for the implementation of the protocol. Since optics facilitates transmission of information from the server to the client and back, we make use of single photonic qubits or a coherent laser beam.

Single photons as information carriers can be described by two quantum fields ($a_0^\dagger$ and $a_1^\dagger$) or states ($|0\rangle$ and $|1\rangle$) and superpositions thereof, such as $(a_0^\dagger + a_1^\dagger)/\sqrt{2}$ or $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Here, the logical states $|0\rangle$ and $|1\rangle$ can, for example, be encoded in the photon's polarization. The operation $U = R_y(\pi/2)$ is a rotation of $\pi/2$ around the Y axis of the Bloch sphere: $R_y(\theta) = \exp(-i\theta/2\sigma_y)$, where σ_y is the Pauli operator, and the bit flip $X = \sigma_X$ is given by the Pauli operator.

However, no quantum behavior is required in our setting. In fact, every system that provides coherence can be used to implement our protocol. In our scenario, using multiple photons, i.e., a product state $|+\rangle|+\rangle\cdots|+\rangle$, also allows the execution of our protocol. The reason for this is that our protocol is only based on classical coherence and the first-order correlation function [17,18], which is the same for true single photons and coherent beams or multiphoton states. This means that the protocol gives the same results for single photons and coherent beams, since higher-order correlation functions, which would show different results for these types of resources, do not play a role in our protocol.

This also means that the protocol we present here is completely classical in the sense of classical physics: it uses purely classical means, effects, and devices, including classical coherence. In a different setting, it could also be accomplished with a classical pointer instead of qubits and coherent beams. Here, the classical pointer represents a three-state system, which can naturally achieve the same functionality as a two-level system with coherence (see Fig. 1). However, this would also require the client to have a different functionality, which would allow the client to compute NAND on her own.

A. Robustness

The challenge when single qubits are used for the protocol is that probabilistic generation and optical losses affect the robustness of the protocol. Since the client is capable of performing only parity computations and preparing random bits, she cannot check whether the computation is correct or not. If the server does not send a photon or the photon gets lost, then the server fails to register a result. The easiest solution would be to send an additional classical bit on a different channel from the server to the client, which indicates that the procedure has worked. Depending on the classical bit, the client could then repeat the computation. However, this is not possible in our framework as this routine would be equivalent to implementing a NAND gate and thus is beyond the client's capabilities. Using a laser beam for the implementation of the protocol has the advantage of providing robustness against these photon losses.

B. Security of implementation

The security of the implemented single-photon protocol follows immediately from the proof given in [8] under two assumptions:

(1) Ideal devices and or devices with noise/loss, provided the noise/loss parameters are not controlled by the server.

(2) The malevolent server sends individual photon states that ensure the operation performed by the client's optical elements on the polarization degrees of freedom of the photons is correct.

Since the security effectively reduces to a classical information-theoretical encryption (effectively a one-time pad) and is not relying on quantum properties vital in most of quantum cryptography (e.g., the no-cloning result for quantum states), having multiple copies of the same state does not reduce the security. The cumulative action of optical devices on the client's side are easily seen to implement a polarization rotation of zero degrees, if $\mathrm{NAND}(a,b) \oplus r = 0$, and π otherwise. In other words, the map itself, implemented by the client, is classically one-time padded. Thus, irrespective of the of the actual state prepared by the server, the action of such a map results in a state that is one-time padded by the parameter r and thus independent of the client's inputs when averaged over the client's secret parameter r. The latter means the protocol is blind.

We note that the security may be jeopardized if the server utilizes other modes, e.g., frequency of light, which changes how the optical devices on the side of the client manipulate the polarization degrees of freedom. However, such behavior can in principle be prevented by quality control, which sporadically checks the characteristics of light used by the server. More general analyses of how particular implementations may be vulnerable to attacks are beyond the scope of this work.

IV. EXPERIMENTS

We implement the server and the client using two independent experimental setups running in two different laboratories which are separated by 50 m (see Fig. 3). We either use a heralded single-photon source or a weak coherent laser beam for the implementation of the protocol. For both cases, we encode the states $|0\rangle$ and $|1\rangle$ in polarization, denoting horizontal and vertical polarization, respectively.

The heralded single photons are produced by type-II parametric down-conversion in a potassium titanium oxide phosphate (KTP) crystal that has periodically poled waveguides [19]. A mode-locked fiber-based femtosecond laser produces 90 -fs-long pulses at 1575 nm with a repetition rate of 100 MHz. These pulses are frequency doubled in a 1-mm-long periodically poled potassium dihydrogen phosphate (KDP) crystal cut for type-II second harmonic generation, resulting in 7 mW of 787.5 -nm light. The fundamental 1575-nm light is filtered out with a dichroic mirror and short-pass filter, and the

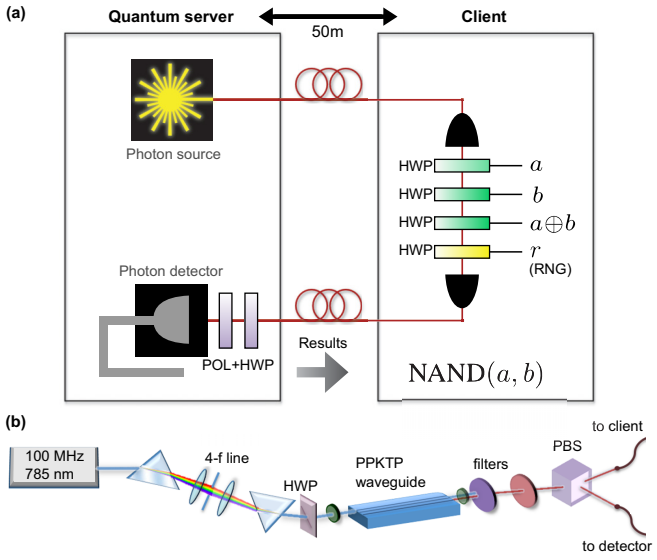

FIG. 3. Experimental setup. (a) Setup of separated client and server. The server in "lab 1" generates and measures polarization-encoded single qubits or the polarization of an attenuated laser beam. The client in "lab 2" manipulates the polarization and encodes the NAND gate. (b) Source for the generation of heralded single photons.

787.5 -nm beam is focused through 3-μm-wide waveguides in a 10 -mm-long AR-coated KTP crystal, which is periodically poled to phase match for type-II parametric down-conversion. After the chip, long-pass filters are used to block out the pump light. The horizontally and vertically polarized down-converted photons, centered at 1570 nm and 1580 nm, are split with a polarizing beam-splitter cube. The photons are further filtered and coupled into single-mode fibers. The photons at 1570 nm are guided to the client's setup, whereas the photons at 1580 nm are kept on the server's side and produce the heralding signal. Alternatively, we use a coherent laser beam at 1550 nm that is attenuated to the single-photon level.

These polarization-encoded cobits are sent to the client who implements the required gates using wave plates. It is sufficient for the client to have access to three half-wave plates (HWPs) for the implementation of the NAND gate and to one additional HWP for the implementation of an additional one-time pad. By applying the following gate sequence,

$$\underbrace{\mathrm{HWP}(\varphi^r)}_{X \text{ or } \mathbf{I}Z} \cdot \underbrace{\mathrm{HWP}(-\theta^{(a\oplus b)}) \cdot \mathrm{HWP}(-\theta^b) \cdot \mathrm{HWP}(\theta^a)}_{\text{gate implementation}}, \quad (4)$$

with $\varphi = \pi/4$ and $\theta = \pi/8$, the client alters the output state, dependent on the values of a and b. The value of the random number r is generated via a classical computer in our implementation. However, this could be easily replaced by a quantum random number generator. The reason for implementing a random X or Z gate instead of X^r is that a real physical implementation introduces state-dependent phase shifts: for the settings $a = b = 0$, $a = 0, b = 1$, $a = 1, b = 0$, the gate sequence $\mathrm{HWP}(-\theta^{(a\oplus b)}) \cdot \mathrm{HWP}(-\theta^b) \cdot \mathrm{HWP}(\theta^a)|0\rangle$ adds an additional phase shift of π to the state $|1\rangle$. This phase shift can be compensated for if we choose to randomly switch between a bit flip X and a phase flip Z in our one-time pad. In order to do so, we use a half-wave plate $\mathrm{HWP}(\varphi^r)$ with $\varphi = \pi/4$. Thus, we can implement the whole scheme using only four HWPs securely [see Eq. (4)].

The output cobit is sent back to the server who performs a measurement in the computational basis. Experimentally, for both implementations, the polarization of the photons returned to the server is analyzed using a half-wave plate, a Glan-Thompson polarizer and InGaAs avalanche photodiodes that are specified to be 20% efficient and a dead time set to 10 μs. The results of the server's measurement is then equal to AND(a,b).

V. RESULTS

We first implement the protocol with single photons. Since the protocol is secure even when multiple photons pass at the same time through the same settings, a single-shot implementation is not necessary and we integrate the result over 10 s of measurement time. In our experiment, we use a Glan-Thompson polarizer and an additional HWP for analyzing the polarization. The results of the single-photon runs are shown in Fig. 4(a). We obtain count rates of 300 heralded photons per second. The average probability for finding the correct results is $(98.8 \pm 0.5)\,\%$.

We run the same experimental sequence with a laser beam that is attenuated to 30 000 single counts per second, measured after the transmission through the setup. In this experimental run, we obtain similar average probabilities of finding the correct results of $(98.2 \pm 0.06)\,\%$. [See detailed results in Fig. 4(b).] In both experiments, the errors are calculated assuming Poissonian errors. Experimental imperfections arise from polarizations drifts when the photons are transmitted through fibers and errors in the manipulations with wave plates as well as imperfection in the measurement in the $|0,1\rangle$ basis.

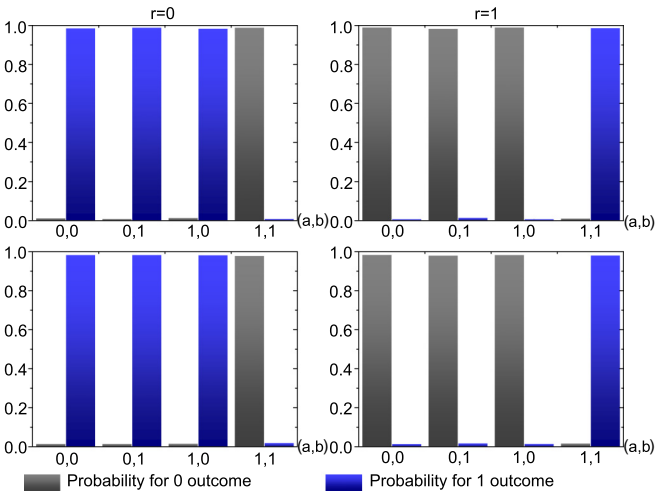

FIG. 4. Results of delegated secure NAND gate. Implementation with single photons (top row) and with an attenuated laser beam (bottom row) for the cases $r = 0$ (left) and $r = 1$ (right). We achieve probabilities for finding the correct output of $(98.8 \pm 0.5)\,\%$ for the single-photon implementation and of $(98.2 \pm 0.06)\,\%$ for the implementation with a coherent beam.

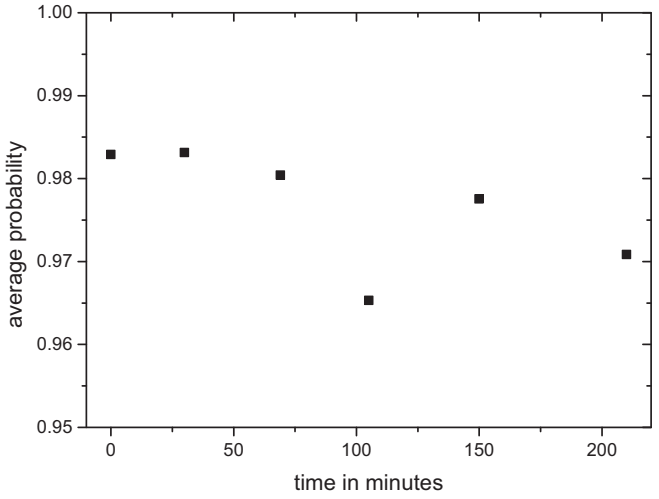

FIG. 5. Study of the long-term stability of our experiment. We repeat the measurement sequence, shown in Fig. 4, six times over 210 min and compute the average probability of obtaining the correct result of the NAND computation (averaged over all results, for $r = 0$ and $r = 1$).

The fibers connecting both laboratories are 50 m long and are placed partly outside the building. In order to test the long-term stability of our fiber connection and influences such as temperature changes and movements of the fibers, we perform a series of NAND-gate measurements for all possible inputs and repeat this measurement six times over 210 min. During this period, the obtained probabilities are stable and decrease only slightly from on average $(98.2 \pm 0.06)\,\%$ to $(97.1 \pm 0.08)\,\%$ (see Fig. 5).

VI. CONCLUSION

We have shown that the computational power of a classical entity limited to parity computations can be boosted to universal classical computation by exploiting coherence. A single qubit can be used as a simple system to accomplish this task—even though no quantumness is required. The extension of previous work to systems capable of being in a coherent superposition of two states provides a practical and robust way to implement the protocol experimentally while still being secure.

While the focus of our work is of a more fundamental nature—demonstrating the computational capability of cobits—a future potential application could be a hybrid quantum-classical secure computing scheme. In such a scheme, a set of NAND gates within a classical circuit may be performed using our protocol. Furthermore, our implementation can be easily extended to long distances using standard technology from quantum key distribution.

In conclusion, our work shows an alternative way of how to exploit the properties of both quantum particles and classical fields as tools for classical computing.

ACKNOWLEDGMENTS

We thank Animesh Datta, Andreas Eckstein, Peter Humphries, Steve Kolthammer, Damian Markham, Ben Metcalf, and Josh Nunn for discussions. This work was supported by the Marie Curie Actions within the Seventh Framework Programme for Research of the European Commission under the Initial Training Network PICQUE, Grant No. 608062, and the European Research Council (ERC) (MOQUACINO), by the European Union's Horizon 2020 Research and Innovation program under Marie Sklodowska-Curie Grant Agreement No. 658073 and by the UK Engineering and Physical Sciences Research Council (EPSRC EP/K034480/1).

[1] R. Rivest, L. Adleman, and M. Dertouzos, Foundations Secure Computation **4**(11), 169 (1978).
[2] C. Gentry, in *Proceedings of the 41st Annual ACM Symposium on the Theory of Computing* (Association for Computing Machinery, New York, 2009), pp. 169–178.
[3] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 2009), pp. 517–526.
[4] S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
[5] T. Morimae, Phys. Rev. A **89**, 060302(R) (2014).
[6] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Phys. Rev. Lett. **111**, 230501 (2013).
[7] K. Fisher, A. Broadbent, L. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. Resch, Nat. Commun. **5**, 3074 (2014).
[8] V. Dunjko, T. Kapourniotis, and E. Kashefi, Quant. Inf. Comput. **16**, 61 (2016).
[9] S.-H. Tan, J. A. Kettlewell, Y. Ouyang, L. Chen, and J. F. Fitzsimons, arXiv:1411.5254.
[10] R. Raussendorf, Phys. Rev. A **88**, 022322 (2013).
[11] J. Anders and D. E. Browne, Phys. Rev. Lett. **102**, 050502 (2009).
[12] K. Loukopoulos and D. E. Browne, Phys. Rev. A **81**, 062336 (2010).
[13] M. J. Hoban, E. T. Campbell, K. Loukopoulos, and D. E. Browne, New J. Phys. **13**, 023014 (2011).
[14] A. Harrow, Phys. Rev. Lett. **92**, 097902 (2004).
[15] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[16] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[17] U. M. Titulaer and R. J. Glauber, Phys. Rev. **145**, 1041 (1966).
[18] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge, UK, 1995).
[19] G. Harder, V. Ansari, B. Brecht, T. Dirmeier, C. Marquardt, and C. Silberhorn, Opt. Express **21**, 13975 (2013).